International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

BPCS Steganography and Visual Cryptography: An Advance Technique for Online Payment Security in E-Commerce for Developing Countries

Vaishnavi J. Deshmukh[1], Dr. A. S. Alvi[2]

[1]M.E Student, CSE Department, Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati. M.S, India

[2]S Associate Professor, Department of CSE, Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati. M.S, India.

Abstract: ***A high-speed prosperity in E-Commerce market has been witnessed in recent time throughout the planet. With ever increasing quality of on-line searching, Debit or mastercard fraud and private data security ar major issues for purchasers, merchants and banks. No institution are left unaffected by the explosion of electronic commerce. although SSL(Secure Socket Layer) is extraordinarily effective and wide accepted because the on-line payment customary, it needs the client Associate in Nursing bourgeois to trust every other: an undesirable demand even in face-to-face transactions, and across the web it admits unacceptable risks. the most motive of this seminar is to produce high level security in E-Commerce applications and on-line searching. this method minimizes elaborate data sharing between client and on-line bourgeois however alter no-hit fund transfer thereby safeguarding client data and preventing misuse of data at merchant's aspect. this is often achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography and Digital Signature for this purpose.***

Keywords: E-Commerce, Online Shopping, Identity Theft, Phishing, BPCS Steganography, Visual Cryptography.

1. Introduction

When you submit your paper print it in two-column format, including figures and tables [1]. In addition, designate one author as the "corresponding author". This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only [2].

2. Existing System

The traditional technique of on-line searching involves client or end-user choosing things on-line searching portal and leading it to the payment entrance. totally {different| completely different} payment gateways have different mechanism of storing careful data of client. There are recent status breaches like in alphabetic character, Sony's PlayStation Network and region Payment Systems show that card holders' data is in danger each from outside and within. the standard system are often graphically expressed in Figure 1:

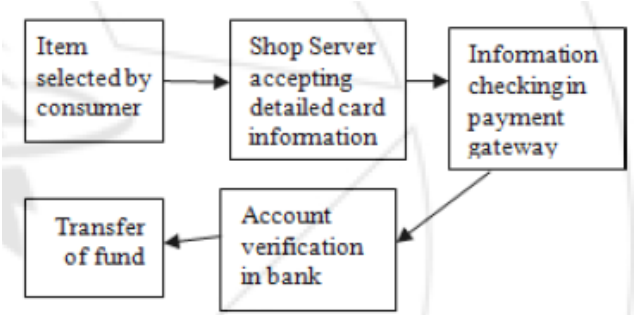

Figure 1: Existing Traditional System

3. Problem Definition

The main motive of the projected system prescribed during this paper is to handle applications that need a high level of security, like E-Commerce applications, core banking and web banking. this could be done by exploitation combination of 2 applications: BPCS Steganography and Visual Cryptography for safe on-line searching and client satisfaction. on-line searching is mostly thought of as retrieval of product data via the web and issue of commercial instrument through electronic purchase request, filling of credit or charge account credit data and shipping of product by order or home delivery by traveler. fraud and phishing area unit the common dangers of on-line searching. fraud is that the stealing of someone's identity within the type of personal data and misuse of that data for creating purchase and gap of bank accounts or transcription credit cards..

4. Proposed System

In this technique, data submitted by the client to the net businessperson is decreased by providing least data which will solely verify the payment created by the same client from its checking account. this can be achieved by the introduction of a central Certified Authority (CA) and combined application of BPCS Steganography and Visual Cryptography. the data received by the businessperson are often within the sort of account range associated with the cardboard used for searching. the data can solely validate receipt of payment from authentic client.

4.1 The BPCS (Bit-Plane quality Segmentation) Steganography formula

The formula are often delineate in compact steps as follows .

1) Convert the carrier image (of any file-format) from PBC (Pure Binary Code) to CGC (Canonical gray Code) system and in png format.
2) Perform the bar chart analysis.
3) After that bit-plane analysis is performed.
4) Perform size-estimation i.e. calculate the places wherever we are able to store the secrete image.
5) Perform bit plane quality segmentation on image i.e. implant secrete blocks into carrier image.
6) After embedding mail that image to a different user.
7) For extracting the embedded image performs de-steganography that is strictly opposite to steganography.

4.2 LinkGuard Algorithm

LinkGuard works by analyzing the variations between the visual link and therefore the actual link. It additionally calculates the similarities of a URI with a far-famed trusty web site [3].

4.3 Proposed Security Architecture for System and its Workflow

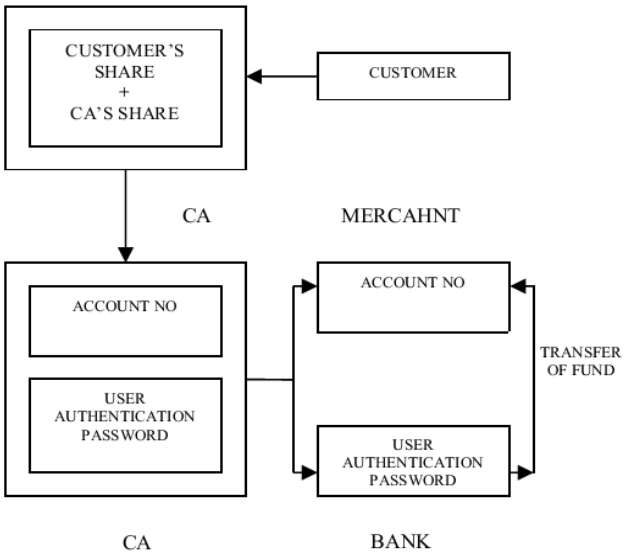

Figure 2: Proposed system Architecture

4.2 Visual Cryptography formula

Visual cryptography may be a sort of cryptography that permits the visual data to be encrypted in suchsome way that their decipherment are often performed by human sensory system.

- each secret element of the first binary image is born-again into four sub element of 2 share picturesand recovered by straightforward stacking method.
- this can be such as exploitation the logical OR operation between the shares .
- Visual cryptography may be a sort of cryptography that permits the visual data to be encrypted in suchsome way that their decryption are often performed by human sensory system.
- each secret element of the first binary image is born-again into four sub element of 2 share pictures and recovered by straight forward stacking method. the 2 apparently random pictures will currently be combined exploitation associate exclusive-or (XOR) to re-create the original image.

4.3 Text primarily based Steganography Methodology

1) Projected text primarily based steganography uses characteristics of West Germanic like inflection, mounted order and use of periphrases for activity information instead of mistreatment properties of a sentence.
2) Variety assignment methodology is employed to maximize no of letters during a specific allotted variety cluster that successively provides flexibility in word selecting and ultimately leads to appropriate sentence construction.

A. Encoding

- Illustration of every letter secretly message by its equivalent code code.
- Conversion of code code to equivalent eight bit binary variety.
- Division of eight bit binary variety into 2 four bit components.
- selecting of appropriate letters from table one appreciate the four bit components.
- purposeful sentence construction by mistreatment letters obtained because the initial letters of appropriate words.
- coding isn't case sensitive.

TABLE I. NUMBER ASSIGNMENT

Letter	*Number assigned*	*Letter*	*Number assigned*
E	15	M	7
A	14	H	7
R	13	G	6
I	13	B	5
O	12	F	4
T	11	Y	4
N	11	W	3
S	10	K	3
L	10	V	3
C	9	X	2
U	8	Z	2
D	8	J	1
P	7	Q	0

Figure 3: Table with number assignment for Cryptography

B. Decoding

- initial letter in every word of canopy message is taken and depicted by corresponding four bit variety.
- bit binary varietys of combined to get eight bit number.
- code codes ar obtained from eight bit numbers.
- Finally secret message is recovered from code codes.

C. Result

To implement the on top of text primarily based steganography methodology, a secret message is taken into account as "text". Text = 01110100011001010111100001110100

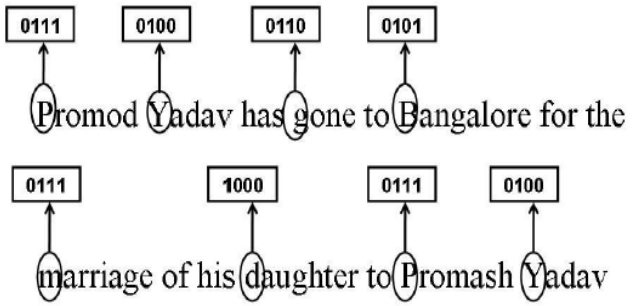

Figure 4: After applying BPCS Steganography

4.4 Visual Cryptography Algorithmic Rule

- Visual cryptography could be a form of cryptography that permits the visual data to be encrypted in such the simplest way that their decryption will be performed by human sensory system.
- each secret constituent of the initial binary image is regenerate into four sub constituent of 2 share pictures and recovered by straightforward stacking method. the 2 apparently random pictures will currently be combined exploitation associate exclusive-or (XOR) to re-create the original image.

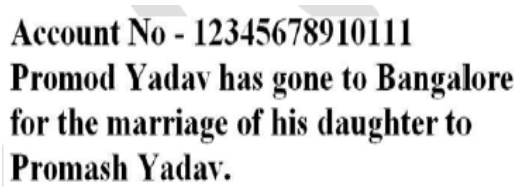

Figure 5: Snapshot Account Number and Cover Text

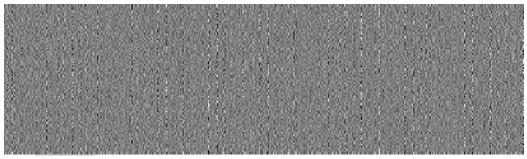

Figure 6: SHARE 1 kept by Customer.

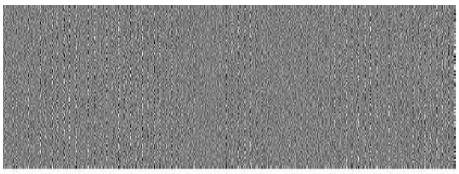

Figure 7:SHARE 1 Kept By Customer

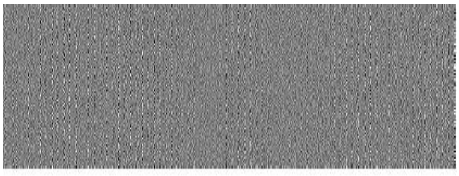

Figure 8: SHARE 2 Kept By Ca

5. Conclusion

In this technique for the protection of on-line payment entryway for E-Commerce, info submitted by the client to the net merchandiser is reduced by providing least info which will solely verify the payment created by the aforementioned client from its checking account. this is often achieved by the introduction of a central Certified Authority (CA) and by combining BPCS Steganography and 2-out-2 visual cryptography that gives client information privacy and prevents misuse of knowledge at merchant's facet. The BPCS Steganography is basically effective against eavesdropping and features a high info activity capability as compared to ancient Steganography approach the data received by the merchandiser may be within the variety of account range associated with the cardboard used for looking the data can solely validate receipt of payment from authentic client. This technique s solely with hindrance of fraud and client information security. the most aim is client satisfaction and approved merchant-bank interaction for fund dealing. as compared to alternative ebanking application that uses BPCS Steganography and Visual Cryptography ar essentially applied for physical banking, the projected methodology may be applied for E-Commerce with focus space on payment throughout on-line looking similarly as physical banking.

6. Advantages

Advantages of BPCS (Bit-Plane complexness Segmentation) Steganography and Visual Cryptography.

- Proposed methodology minimizes customer's elaborated info sent to the web merchandiser. Thus although a breach takes place in merchant's information, client doesn't get affected.
- Certified Authority acts as a fourth party thereby enhancing customer's satisfaction and security more.
- Usage of BPCS Steganography ensures that the CA doesn't apprehend client authentication watch word so maintaining client privacy. It provides a better level of security and a high info concealment capability.
- Since client knowledge is distributed over three parties, a breach in single information will simply be self-satisfied.
- The 2-out-2 feature of visual cryptography provides effective collaboration of pictures at the Certified Authority's facet.

7. Future Scope

The payment system may also be extended to web or physical banking. Shares might contain client image or signature additionally to client authentication word. within the bank, client submits its own share and client physical signature is valid against the signature obtained by combining client's share and CA's share at the side of validation of customer authentication word. It prevents misuse of taken card and stops illegitimate client. this will be additionally applied for standardization of a selected product or a company by having their personal identification secured.

References

[1] Souvik Roy, P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014.

[2] Pranita P. Khairnar, Prof. V. S. Ubale, " Steganography Using BPCS technology,"in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.
[3] U.Naresh, U.Vidya Sagar, C.V. Madhusudan Reddy , " Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36.
[4] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.
[5] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
[6] ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,",in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008.

Author Profile

Vaishnavi J.Deshmukh has received her B.E.(Computer Sci. & Engg) from SGBAU Amaravati University and currently pursuing her M.E in Comp Sci. & Engg from SGBAU Amaravati University, Currently working with GRWPY Yavatmal as a Lecturer. Her area of interest focus on E-Commerce Security, System Security.

Dr. A.S.Alvi has received his M.E. in Computer Sci. & Engg and also completed his Ph.D in Computer Sci & Engg. Currently working with PRMITR, Badnera, Amravati as an Associate Professor. He has 20 years of teaching experience . He has Professional Memberships : Life Member Of The Indian Society For Technical Education(LM-12323) Member of the Institute of Engineers (India) (M127698/5)